NOTICES *

**JPO and INPIT are not responsible for any damages caused by the use of this translation.**

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

## DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to a server for access controls, a disc array system, and an access control method for the same.
[0002]
[Description of the Prior Art]In recent years, the amount of information treated with the computer system used in a company etc. is increasing by leaps and bounds.
The increase also of capacity, such as a disk unit which memorizes data in connection with this, is being enhanced.
A device with the capacity of several TB (terabyte) is also becoming for example, less new in a magnetic disk drive. It is indicated by the patent documents 1 about rearrangement of the logical disk device which one set of a memory control unit has managed, concerning such a disk unit. A logical disk device with high access frequency is specifically rearranged to a more nearly high-speed physical disk device by judgment of a customer engineer based on access information, Rearranging a logical disk device with a high ratio of a sequential access to a physical disk device with higher sequential access performance is indicated.
[Patent documents 1] JP,H9-274544,A[0003]
[Problem(s) to be Solved by the Invention]Assigning memory storage per a user unit or host is not indicated by the above-mentioned conventional technology.
[0004]That is, if the capacity of memory storage increases, in order to use the memory storage effectively, it is possible [ it ] to share by two or more users. In SSP (Storage Srevice Provider) etc., it is possible to offer service which divides memory storage into some Types and uses it. In such a case, quota ****** is [ administrator ] needed in the field of memory storage per a user unit or host. in order for a quota **** user to use the field effectively, other users need to enable it to use a certain field
[0005]This invention was made in view of such SUBJECT, and assigns a storage area to a user

or a host, and also an object of this invention is to provide the method or device which can set the access permission to the storage area as a user unit or a host unit.
[0006]
[Means for Solving the Problem]That said purpose should be attained in a main invention of this invention. If access from a user to two or more disk units is managed and a demand of said access to said logical volume is received from said each user, Based on information on the right to access defined for every user, a judgment of either permission or disapproval is made to said access about each logical volume which said each disk unit memorizes.
[0007]
[Embodiment of the Invention]With reference to Drawings, it explains about a server for access controls concerning an embodiment of the invention, a disc array system, and an access control method for the same. Drawing 1 shows the block diagram of the whole system, and has two or more data-access hosts 400, the administrative client 500, the server 300 for access controls, two or more disk array devices 200, and the switch 600. The data-access host 400, the administrative client 500, the server 300 for access controls, the disk array device 200, and the switch 600 are connected, for example by the network by an IP protocol. The data host 400, the switch 600, and the disk array 200 are connected to the network by a fiber channel protocol. In drawing 1, the interface with the network according an interface with the network of an IP protocol to "IF" and a fiber channel protocol is shown as "FCIF." The disk array device 200 and the system constituted by the server 300 for access controls are called a disc array system.
[0008]The disk array device 200 comprises a RAID (Redundant Array for Inexpensive Disk) device. The server 300 for access controls manages access from the user to the disk array device 200.
[0009]The data-access host 400 has the following.
It is a server machine using the logical volume of the disk array device 200, and is the memory 440.
CPU430 which executes the program stored in the memory.
The host agent's 410 program and the access restriction information 420 are stored in the memory 440.
[0010]The administrative client computer 500 is provided with the following.
Memory 530.
CPU520 which executes the program stored in the memory 530.
The program of administrative UI(User Interface, console) 510 is stored in the memory 530. This administrative UI510 notifies information, including ID etc. which a user (storage manager) inputs, to the server 300 for access controls. Based on the operational input which led administrative UI510 of the user (storage manager), the administrative client computer 500 defines the composition of logical volume, or sets up a user's access right.
[0011]The RAID device which constitutes the disk array device 200 is a disk storage device which has a function with which the data-access host 400 is provided by making 1 or two or more volumes into a logical storage area. The disk array device 200 has two or more disk units

210, the control section 240, and the memory 230. The volume configuration information 220 by which the composition of logical volume was defined is stored in the memory 230.
[0012]The server 300 for access controls can control setting out of the volume configuration information 220 in the disk array device 200, and the switch 600, and can perform control of the path of a data access, etc. Specifically, this server 300 for access controls has CPU301 and the DB (database) section 350 which execute the program stored in the memory 302 and the memory 302. Programs, such as the user authentication module 330, the access control module 320, the RAID constitution administrative module 310, and the switch control module 340, are stored in the memory 302.
[0013]The user authentication module 330 attests the user who logged in through the data-access host 400 and the administrative client computer 500. The information ("User Information 370" is only called hereafter.) about a user required for this attestation is acquired from DB part 350.
[0014]The access control module 320 judges either permission or disapproval to a user's access based on the information on the right to access stored in DB part 350 ("the access right information 380" is only called hereafter.).
[0015]The RAID constitution administrative module 310 sets the volume configuration information 220 which acquired the volume configuration information 220 from the disk array device 200, and was defined as the disk array device 200.
[0016]The switch control module 340 enables it to perform the data access to logical volume, when the access control module 320 grants a permission. In response to permission of the access control module 320, specifically, the switch control module 340 sends the switch information 390 to the switch 600, in order to set a path.
[0017]The information ("the configuration information 360" is only called hereafter.) about the composition of the logical volume defined by the volume configuration information 220 on the disk array device 200 is stored in DB part 350. As this DB350 was mentioned above, User Information 370 required for a user's attestation and the switch information 390 for setting the path of the access right information 380 defined for every user about each logical volume and a switch are stored.
[0018]An example of the concrete contents of configuration information mentioned above is explained with reference to the table showing the configuration information on drawing 2. As an item of configuration information, as shown in drawing 2, each ID (logical volume ID) of each logical volume is received, Respectively, the address of the ports ID (port address) and LUN (Logical Unit Number), a device number (LDEV, Logical Device Address), and a disk array device, etc. are given. Logical volume ID is ID the data-access host (server) 400 indicates accessible logical volume (logical storage volume) to be. The ports ID and LUN and a device number are used for the data-access host's 400 access. And these information is managed to all the disk array devices used as an administration object.
[0019]An example of the concrete contents of User Information 370 mentioned above is explained with reference to the table showing User Information of drawing 3. As an item of this User Information, as shown in drawing 3, the right to access as a host address, a password, and

each user's role, etc. are given to each ID (user ID) of a user, respectively. A host address is a physical address (World Wide Name) given to the data-access host 400 whom a user uses. Two or more definitions are possible for this physical address to one user ID. For example, the "SSP (Storage Service Provider) administration right" is defined as two addresses "01230", "02345", a password, and the right to access to the user ID "Na" of the party eye in the table of drawing 3. The whole (all the logical volume which the disk array device 200 managed by the server 300 for access controls has) resource of SSP is received as indicated as the SSP administration right in the column of explanation of drawing 3, It means that the power of full access without restriction is lodged. Other user ID is as having been indicated on the table of drawing 3.

[0020]An example of the concrete contents of the access right information 380 mentioned above is explained with reference to the access control table showing the access right information of drawing 4. As an item of this access right information, as shown in drawing 4, the access right information (logical volume **** setting-out authority information is included) about each logical volume is given to each user, respectively.

[0021]For example, the user ID of the 1st row of the table of drawing 4 "Na" is an SSP administrator. For this reason, user ID "Na" has the authority to refer to and ("in figure R") change the definition of that composition ("Xin figure"), to all the storage resources (Vol-0 thru/or Vol-5). Namely, as for user ID "Na", setting out of a definition of logical volume is considered as permission about Vol-0 thru/or Vol-5. On the other hand, it does not have the reference ("in read-out, transmission, and figure r") to the data of logical volume itself, and the authority to write in ("in figure w") (inside of a figure "-- RX"). That is, user ID "Na" lets access (data access) be disapproval about Vol-0 thru/or Vol-5.

[0022]The user ID of the 2nd row of the table of drawing 4 "Ha" is the administrator of the whole storage resource (Vol-0, Vol-1) to whom A company was assigned as the "A company aa" and the "A company ab." For this reason, while user ID "Ha" has the authority to refer to and ("in figure R") change the definition of that composition ("Xin figure"), about logical volume Vol-0 and Vol-1, It has reference ("in figure r"), and the authority to write in ("in figure w") also to the data of logical volume itself ("rwRXin figure"). That is, as for user ID "Ha", access (data access) is considered as permission about Vol-0 and Vol-1. This user ID "Ha" cannot perform all accesses, such as reference, change, and writing, about any logical volume (Vol-2 thru/or Vol-5) other than a its company slack A company (inside of a figure "----"). Namely, as for user ID "Ha", let setting out of a definition of logical volume be disapproval about Vol-2 thru/or Vol-5.

[0023]The user ID of the 3rd row of the table of drawing 4 "Ka" is an administrator of aa section of A company. For this reason, while user ID "Ka" has the authority to refer to and ("in figure R") change the definition of that composition ("Xin figure"), only about logical volume Vol-0 assigned to aa section, It has reference ("in figure r"), and the authority to write in ("in figure w") also to the data of logical volume itself ("rwRXin figure"). This user ID "Ka" cannot perform all accesses, such as reference, change, and writing, about any logical volume (Vol-1 thru/or Vol-5) other than a self-section company slack aa section (inside of a figure "----").

[0024]The user ID of the 5th row of the table of drawing 4 "Ue" is a general user of ab section of

A company, and is not an administrator further again. For this reason, user ID "Ue" only about logical volume Vol-1 assigned to ab section. While it has reference ("in figure r"), and the authority to write in ("in figure w") also to the data itself, it does not have the authority to refer to and change the definition of the composition ("rw in a figure -- ").

## CLAIMS

[Claim(s)]
[Claim 1]Information on logical volume which is a server for access controls which manages access to two or more disk units, and said each disk unit memorizes and which was divided logically, A server for access controls sending information about logical volume to which setting out of the right to access was permitted based on a user's sent identifier from memory storage with which information to which setting out of the right to access to logical volume is permitted for every identifier of a user was memorized.
[Claim 2]Structure definition information which matched logical volume and a host address from information on the right to access to sent logical volume in a server for access controls indicated to Claim 1 is generated, A server for access controls sending generated structure definition information to a disk unit in which a physical disk corresponding to the logical volume concerned exists.
[Claim 3]A server for access controls characterized by comprising the following.
Information on the right to access defined for every identifier of each user about logical volume which is a server for access controls which manages access from a user to two or more disk units, and said each disk unit memorizes, and which was divided logically.
An access control means which will make a judgment of either permission or disapproval to said access based on a user's identifier and information on said right to access if a demand of said access to said logical volume is received.

[Claim 4]Said access is a definition of said logical volume access for setting up, and information on said right to access, Logical volume definition setting-out authority information which shows either permission or disapproval about setting out of a definition of said logical volume which is an object of said access is included, The server for access controls according to claim 3, wherein said access control means makes setting out of a definition of said logical volume permission or disapproval based on said logical volume definition setting-out authority information.
[Claim 5]The server for access controls according to claim 4 provided with a logical volume definition setting-out execution means by said access control means which performs this setting out according to a result of judgment which makes setting out of a definition of said logical volume permission or disapproval.
[Claim 6]The server for access controls according to claim 3, wherein said access is provided with a pass control means which is access to data of said logical volume, and enables this access to a demand of said access based on a result of judgment of said access control means.
[Claim 7]A disk array device which has two or more disk units.
A server for access controls which manages access from a user to said disk array device.
Are the above the disc array system which it had, and said server for access controls, If it has the information on the right to access defined for every identifier of each user about each logical volume which said each disk unit memorizes and a demand of said access to said logical volume

is received, Based on said user's identifier, and information on said right to access, it had an access control means which makes a judgment of either permission or disapproval to said access.

[Claim 8]Said access is access for setting up a definition of said logical volume, and information on said right to access includes logical volume definition setting-out authority information which shows either permission or disapproval about setting out of a definition of said logical volume which is an object of said access.
The disc array system according to claim 7, wherein said access control means makes setting out of a definition of said logical volume permission or disapproval based on said logical volume definition setting-out authority information.

[Claim 9]The disc array system according to claim 8 provided with a logical volume definition setting-out execution means by said access control means which performs this setting out according to a result of judgment which makes setting out of a definition of said logical volume permission or disapproval.
[Claim 10]The disc array system according to claim 7, wherein said access is provided with a pass control means which is access to data of said logical volume, and enables this access to a demand of said access based on a result of judgment of said access control means.
[Claim 11]If it is the method of managing access from a user to two or more disk units and a demand of said access to said logical volume is received from said each user, An access control method making a judgment of either permission or disapproval to said access based on information on the right to access defined for every identifier of each user about each logical volume which said each disk unit memorizes.
[Claim 12]Said access is access for setting up a definition of said logical volume, and information on said right to access includes logical volume definition setting-out authority information which shows either permission or disapproval about setting out of a definition of said logical volume which is an object of said access.
The access control method according to claim 11 characterized by making setting out of a definition of said logical volume into permission or disapproval based on said logical volume definition setting-out authority information.

[Claim 13]A method for access controls according to claim 12 characterized by performing this setting out according to a result of judgment which makes setting out of a definition of said logical volume permission or disapproval.
[Claim 14]Are the method of managing access to two or more disk units, and based on a user's sent identifier, An access control method specifying information on logical volume that setting out of the right to access was permitted to an identifier of the user concerned, and setting up an identifier of a user who can set up the right to access to said specified logical volume.

## DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a block diagram showing the entire configuration containing a storage system.
[Drawing 2]It is a chart showing the table about an example of the configuration information on the logical volume with which a disk array device is provided.
[Drawing 3]It is a chart showing the table of an example of User Information with which a disk array device is provided.
[Drawing 4]It is a chart showing the access control table showing an example of the access right information with which a disk array device is provided.
[Drawing 5]It is a chart showing the table showing an example of switch information used with an access control method.
[Drawing 6]It is a figure showing operation of the whole system.
[Drawing 7]It is a flow chart which shows the first working example of an access control method.
[Drawing 8]It is a figure showing an example of a screen which defines the configuration change to logical volume.
[Drawing 9]It is a figure showing an example of a screen which sets up the right to access to logical volume.
[Drawing 10]It is a chart showing the volume configuration information used with an access control method.
[Drawing 11]It is a chart showing the access restriction information by which logical volume and its authority were defined.
[Drawing 12]It is a flow chart which shows the second working example of an access control method.
[Drawing 13]It is a flow chart which shows the third working example of an access control method.
[Description of Notations]
100 Disc array system
200 Disk array device
210 Disk unit
220 Logical organization control section
300 The server for access controls
310 User authentication part
320 Access control section
330 RAID constitution Management Department
340 Pass control part
350 DB part
400 Data-access host
410 Host agent part
500 Administrative client computer
510 Administrative UI section

## DRAWINGS

[Drawing 2]

図2

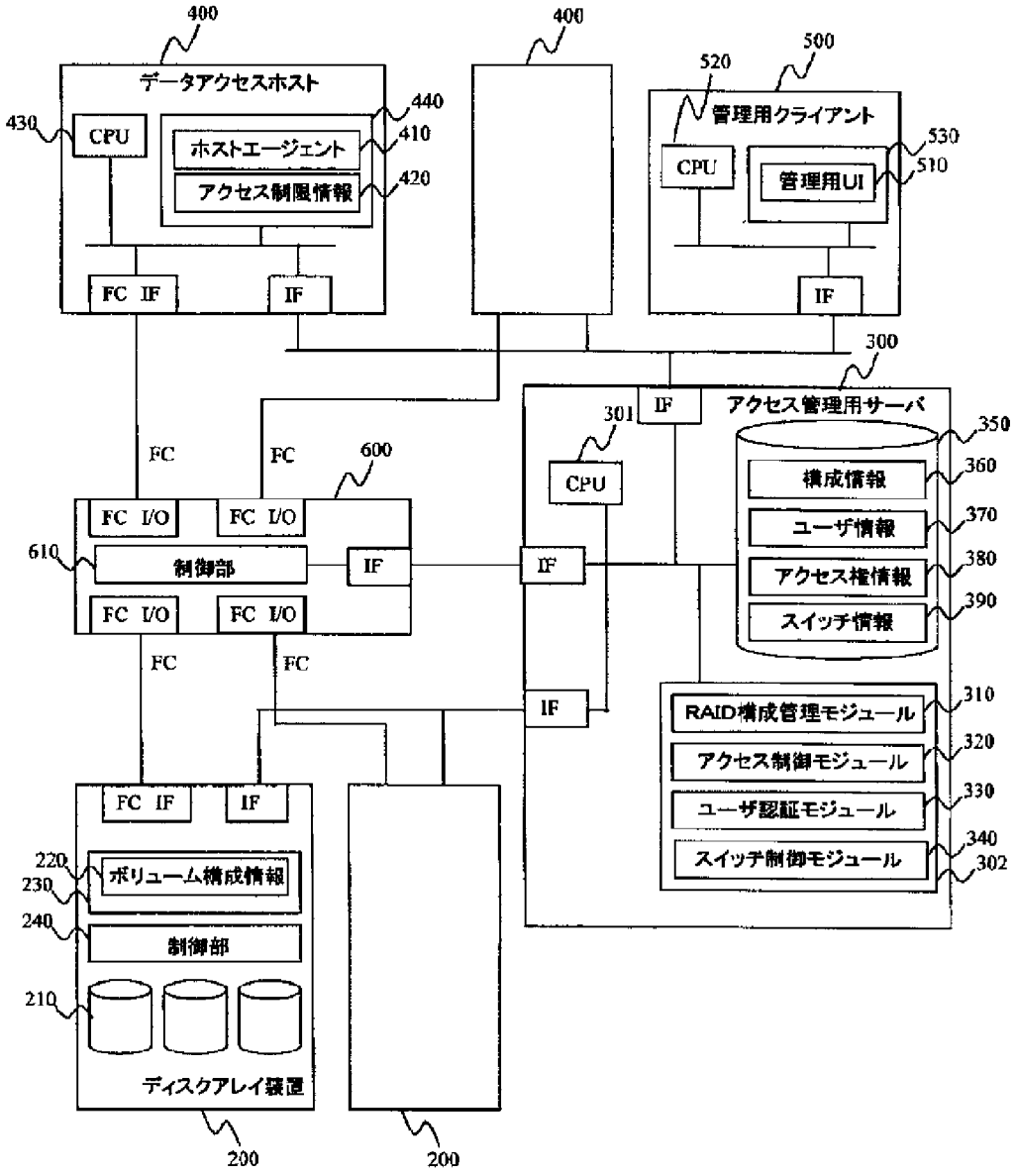
| 論理ボリュームID | ポートID | LUN | デバイス番号 (CU:LDEV) | ディスクアレイ装置アドレス | |
|---|---|---|---|---|---|
| Vol-0 | CL0-A | 0 | 0:1E | 0001 | |
| Vol-1 | CL0-A | 1 | 0:1F | 0001 | |
| Vol-2 | CL0-B | 0 | 0:2D | 0001 | |
| Vol-3 | CL0-A | 1 | 0:2C | 0001 | |
| Vol-4 | CL0-B | 0 | 0:40 | 0002 | |
| Vol-5 | CL0-A | 1 | 0:40 | 0002 | |
| | | | | | |

[Drawing 5]

【図5】

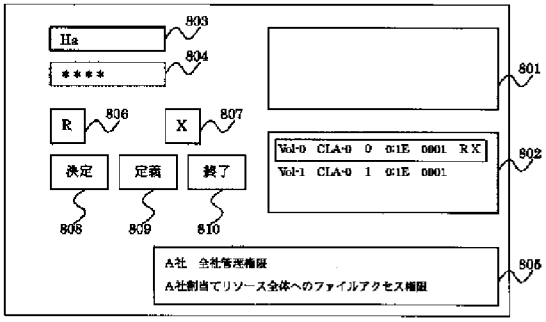
| ポート | ゾーン定義 |
|---|---|
| Port A | ゾーン1 |
| Port B | ゾーン2 |
| Port C | ゾーン1 |
| Port D | ゾーン2 |

[Drawing 1]
【図１】


400
データアクセスホスト
430
CPU
440
ホストエージェント
410
アクセス制限情報
420
FC IF
IF
400
500
520
管理用クライアント
CPU
530
管理用UI
510
IF
300
アクセス管理用サーバ
301
IF
CPU
350
構成情報
360
ユーザ情報
370
アクセス権情報
380
スイッチ情報
390
FC
FC
600
FC I/O
FC I/O
610
制御部
IF
FC I/O
FC I/O
FC
FC
IF
RAID構成管理モジュール
310
アクセス制御モジュール
320
ユーザ認証モジュール
330
スイッチ制御モジュール
340
302
FC IF
IF
220
ボリューム構成情報
230
240
制御部
210
ディスクアレイ装置
200
200

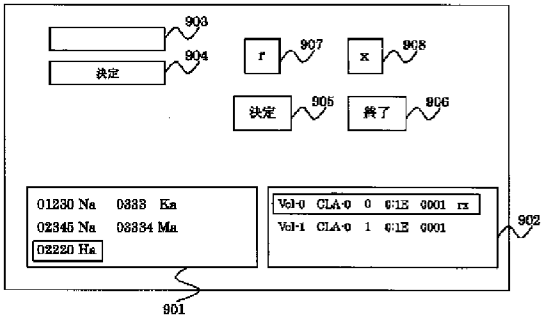
[Drawing 8]

図８




[Drawing 9]

図９




[Drawing 3]

【図３】

ユーザ情報

| ユーザID | ホストアドレス | パスワード | 権限 | 説明 |
|---|---|---|---|---|
| Na | 01230<br>02345 | * *<br>* | SSP 管理権限 | SSP のリソース全体へのフルアクセス権限 |
| Ha | 02220 | * *<br>* | A社 全社管理権限 | A社割当てリソース全体へのフルアクセス権限 |
| Ka | 0333 | * *<br>* | A社 aa部門管理権限 | A社の aa 部門のリソースへのフルアクセス権限 |
| Ma | 03334 | * *<br>* | A社 ab部門管理権限 | A社の ab 部門のリソースへのフルアクセス権限 |
| Ua | 03370 | * *<br>* | A社 ab 部門一般権限 | A社のab部門の一般ユーザアクセス権限 |
| Ho | 05556 | * *<br>* | B社 全社管理権限 | B 社管割当て全リソースへのフルアクセス |
| Ta | 05569 | * *<br>* | B社 bb/bc 部門管理権限 | B社の bb/bc 部門のリソースへのフルアクセス |
| Ok | 05551 | * *<br>* | B社 bb部門管理者権限 | B社の bb 部門割当てリソースへのフルアクセス |
| Ba | 05551 | * *<br>* | B社 bb 部門一般権限 | B社のbb部門の一般ユーザアクセス権限 |
| Ka | 05558 | * *<br>* | B社 bc部門管理権限 | B社のbc部門割当てリソースへのフルアクセス |
| Sh | 05606 | * *<br>* | B社 bc 部門一般権限 | B社のbd部門の一般ユーザアクセス権限 |
| : | : | : | : | : |
| | | | | |

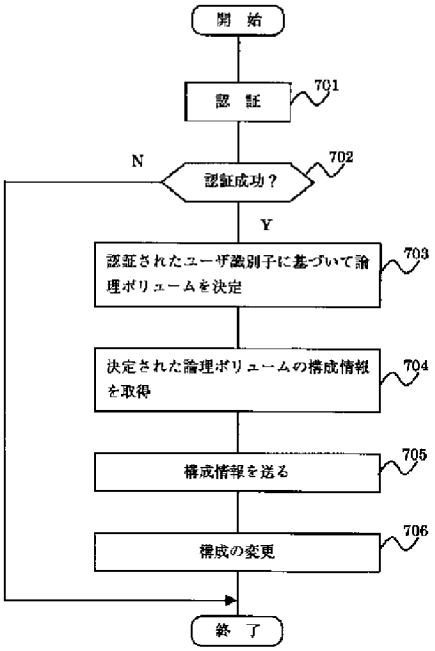
[Drawing 4]
【図４】

アクセス管理テーブル

| | | 論理ボリューム | | | | | |
|---|---|---|---|---|---|---|---|
| | | Vol-0 | Vol-1 | Vol-2 | Vol-3 | Vol-4 | Vol-5 |
| ユーザ | Na | --RX | --RX | --RX | --RX | --RX | --RX |
| | Ha | rwRX | rwRX | ---- | ---- | ---- | ---- |
| | Ka | rwRX | ---- | ---- | ---- | ---- | ---- |
| | Ma | ---- | rwRX | ---- | ---- | ---- | ---- |
| | Ue | ---- | rw-- | ---- | ---- | ---- | ---- |
| | Ho | ---- | ---- | rwRX | rwRX | rwRX | ---- |
| | Ta | ---- | ---- | rwRX | rwRX | ---- | ---- |
| | Ok | ---- | ---- | rwRX | ---- | ---- | ---- |
| | Ba | ---- | ---- | rw-- | ---- | ---- | ---- |
| | Ka | ---- | ---- | ---- | rwRX | ---- | ---- |
| | Sh | ---- | ---- | ---- | ---- | rw-- | ---- |
| | : | | | | | | |
| | | A社 aa | A社 ab | B社 bb | B社 bc | B社 bd | — |

凡例：r(データの参照権限)、w(データの書込み権限)、R(構成情報の参照権限)、X(構成定義の変更やボリューム削除などの管理権限)、－(権限無し)

[Drawing 7]
図７



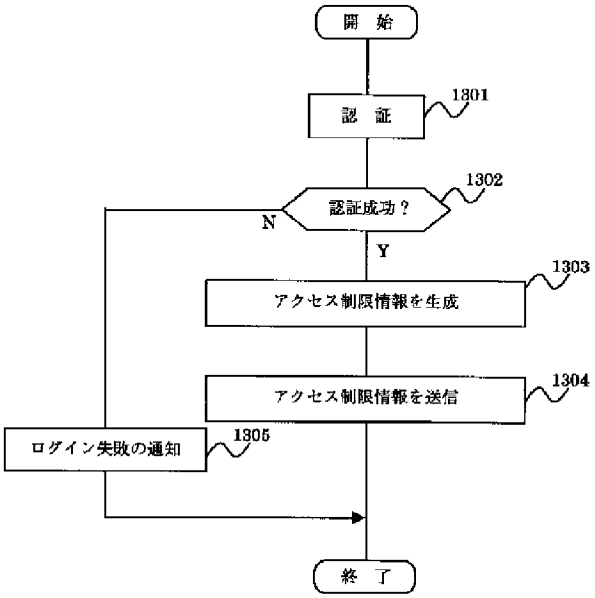

[Drawing 10]
【図１０】

| 論理ボリュームID | ポートID | LUN | デバイス番号 (CU:LDEV) | ホストアドレス |
|---|---|---|---|---|
| Vol-0 | CL0-A | 0 | 0:1E | 02220 |
| Vol-1 | CL0-A | 1 | 0:1F | 02220 |
| Vol-2 | CL0-B | 0 | 0:2D | |
| Vol-3 | CL0-A | 1 | 0:2C | |
| Vol-4 | CL0-B | 0 | 1:40 | |
| Vol-5 | CL0-A | 1 | 1:40 | |
| | | | | |

[Drawing 11]
【図１１】

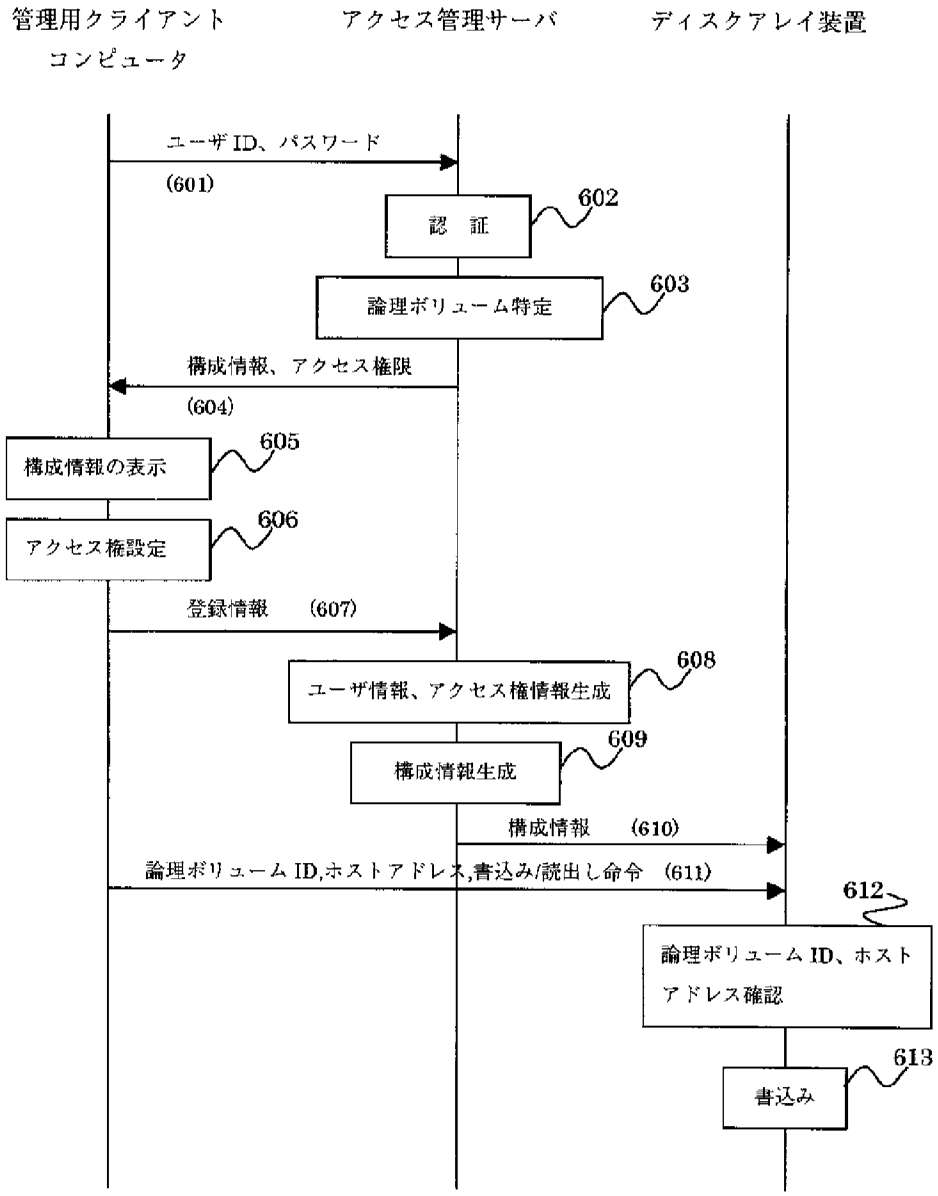
| 論理ボリュームID | 権限 |
|---|---|
| Vol−0 | rw |
| Vol−1 | rw |

[Drawing 13]
図１３



[Drawing 6]

図 6


管理用クライアント
コンピュータ
アクセス管理サーバ
ディスクアレイ装置
ユーザ ID、パスワード
(601)
認　証
602
論理ボリューム特定
603
構成情報、アクセス権限
(604)
構成情報の表示
605
アクセス権設定
606
登録情報　(607)
ユーザ情報、アクセス権情報生成
608
構成情報生成
609
構成情報　(610)
論理ボリューム ID,ホストアドレス,書込み/読出し命令　(611)
612
論理ボリューム ID、ホスト
アドレス確認
613
書込み

[Drawing 12]

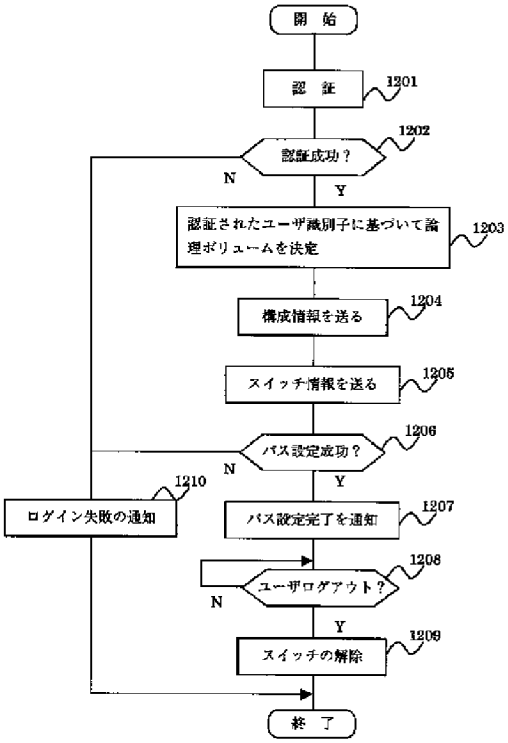



図１２